STATE OF VERMONT
Agency of Administration

POLICY MANUAL **IRMAC** **INFORMATION RESOURCE MANAGEMENT ADVISORY COUNCIL**	**ORIGINAL POLICY ADOPTED BY IRMAC** **DATE: 03/17/2000**	**ORIGINAL POLICY NUMBER**
	EFFECTIVE DATE **03/17/2000**	**IDENTIFIER** REV C 12/10/2001

STATUTORY REFERENCE OR
OTHER AUTHORITY:

APPROVAL DATE: 03/17/2000

APPROVED BY:

POLICY TITLE: **Security Intrusion Policy**

POLICY STATEMENT:

Vermont State Government relies on desktop computers, servers, LAN's and WAN's as well as the Intranet\Internet for day-to-day business. Network accessibility depends on complex systems that may be targets of malicious and/or criminal activity.

All government entities shall take precautions against intrusions to their computing and communication infrastructure. This should include the monitoring of systems under their jurisdiction and the capability to identify and report breaches that occur.

IRMAC will establish procedures and reporting protocol and set such guidelines as required to implement this policy. Please refer to the Incident Handling Procedure when enforcing this policy.

A Computer Security Incident Response Team (CSIRT) is hereby created. This team of technical professionals will provide a central coordination center, with a single point of contact for computer security issues. The Team shall be composed of a member from GovNet, the Assistant CIO or CIO, Director of CIT and two departmental representatives. (**Membership on this team is in addition to normal duties of their position**).

CSIRT:
The overall goal is a safe and secure technical environment for the purpose of conducting government business. CSIRT will achieve this goal by providing:

- Single point of contact for security issues and guidance
- A coordinated response among system administrators, investigators and law-enforcement to a reported incident
- Liaison to other CSIRTs in both the private and public sectors
- Coordination of services which improve security and minimize the threat of damage from intrusions
- Performing periodic network vulnerability assessments
- Distribution of information to all staff that recognizes that prevention, and not simply detection, is key to thwarting attackers